



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/600,297	07/13/2000	JIAN HU	13267.2USWO	2701
23552	7590	06/03/2005	EXAMINER	
MERCHANT & GOULD PC				TRUONG, THANHNGA B
P.O. BOX 2903				
MINNEAPOLIS, MN 55402-0903				
ART UNIT		PAPER NUMBER		
2135				

DATE MAILED: 06/03/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/600,297	HU ET AL.
	Examiner Thanhnga B. Truong	Art Unit 2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 3/9/2005 (RCE).
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-33 and 35 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-33 and 35 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on 13 July 2000 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
 Paper No(s)/Mail Date _____

4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____
 5) Notice of Informal Patent Application (PTO-152)
 6) Other: _____

DETAILED ACTION

1. Applicant's submission for RCE filed on March 09, 2005 has been entered. Claims 1-33 and 35 are pending.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Turk et al (US 5, 983,207), and further in view of Yasukawa et al (US 5,999,622).

a. Referring to claim 1:

i. Turk teaches:

(1) digital data storage means [i.e., referring to Figure 1, one storage site, that is “data storage means”, is a secure facility (e.g., a vault) in which the valuable commodity is held for safekeeping (column 4, lines 6-8)];

(2) a user account associated with the user [i.e., referring to Figure 1, customer(i) 10, that is “a user account”, stores gold at a storage site 12 (column 7, lines 2-3)]; and

(3) means for establishing a digital data transaction session in which the user is able to instruct storage or retrieval of a digital data item in association with the user's account [i.e., referring to Figure 1, customer(i) 10 stores gold at a storage site 12 and requests the storage site to send him ecoins (e.g., digital data, the electronic representation of a valuable commodity, preferably, a precious metal such as gold, platinum, palladium, or silver, which is held for safekeeping at a storage site). The storage site contacts the emint 14 and informs it of the receipt of new gold (column 7, lines 1-6)];

(4) means for encoding the data item into a plurality of parts, the parts being separately stored in the storage means [i.e., each ecoin may

appear as a string of alphanumeric characters which may also be encrypted and/or digitally signed for security (column 3, lines 50-52)]; and

(5) means for decoding the encoded data item to retrieve the data item from the separately stored parts, whereby the data item is retrievable even if some of the parts are lost or corrupted[i.e., "private key" is a mathematical key which is kept private to the owner and which is used to create digital signatures, and in the context of encrypted communications, is used to decrypt electronic data encrypted with the corresponding public key (column 4, lines 1-5)].

ii. Although Turk teaches ecoin to be encrypted for security, Turk is silent about encrypting ecoins into a plurality of parts or portions or segments and storing them separately in storage sites. On the other hand, Yasukawa teaches:

(1) The encrypted digital information is stored in a file, but individual segments of data which make up the file are encrypted according to some chosen encryption pattern. The data segments encrypted represent logical segments corresponding to an actual portion of the physical media on which the file is stored (e.g. sectors on a CD-ROM, hard disk, a memory block, etc). The encrypted information includes data indicating the original proprietor of the original digital information (i.e. the original file in which the digital information is stored) (**column 3, lines 43-52**).

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have applied the teaching of Yasukawa into Turk's system since using more than one encryption scheme changes the "depth" of the encryption segment providing additional protection to a portion of valuable data (**column 3, lines 59-62 of Yasukawa**).

iv. The ordinary skilled person would have been motivated to:

(1) have applied the teaching of Yasukawa into Turk's system because data is encrypted on a per-sector basis. Some portion of a sector comprising a file can be left unencrypted, speeding access since less decryption is required. Different files can utilize different encryption depth techniques, increasing

protection against unauthorized decryption (**column 1, lines 66-67 through column 2, lines 1-4 of Yasukawa**).

b. Referring to claim 2:

i. Turk further teaches:

(1) wherein the data storage means comprises at least one data storage device, the parts being separately stored on the data storage device or devices [**i.e., a "storage site" as used herein is a secure facility (e.g., a vault) in which the valuable commodity (e.g., gold) is held for safekeeping. Preferably there are several storage sites for storing the commodity, that is "the parts being separately stored on the data storage device or devices" (column 4, lines 6-9)**].

c. Referring to claim 3:

i. Turk further teaches:

(1) means for communication with the user [**i.e., referring to Figure 1, customer(i) 10 stores gold at a storage site 12 and requests the storage site to send him ecoins (e.g., digital data, the electronic representation of a valuable commodity, preferably, a precious metal such as gold, platinum, palladium, or silver, which is held for safekeeping at a storage site). The storage site contacts the emint 14 and informs it of the receipt of new gold (column 7, lines 1-6)**].

d. Referring to claims 4, 5:

i. Turk further teaches:

(1) means for authentication of the user with the depository; means for authentication of the depository by the user [**i.e., "digital signature" is information generated by a private key applied and appended to electronic data. If the electronic data is not altered after the digital signature has been applied, the signature will verify the authenticity of the electronic data when checked with the corresponding public key (column 3, lines 35-40). The "emint" is a computer and communications system which creates, distributes and verifies the authenticity of ecoins, and which receives information from the storage sites**]

regarding gold held there for storage and specifically identified for use in the digital cash system (column 4, lines 45-59)].

e. Referring to claims 6, 7, and 8:

i. Turk further teaches:

(1) wherein the user is able to instruct retrieval of a copy of the item in said transaction session; wherein the user is able to instruct deletion of the digital data item in said transaction session; wherein the user is able to instruct an account status report in said transaction session [i.e., the system of the invention requires some system users to establish a fiduciary relationship with a storage site. The relationship is confirmed when a system user either (1) stores gold with, or (2) purchases from another person gold already held at one or more storage sites. In the first case, the storage site verifies the receipt of the gold and provides confirmation to the system user specifying the pure weight and/or other physical attributes of the gold. In the second case, the storage site records the transfer of gold from one system user to the other (column 4, lines 50-59). Furthermore, "client software" is a software application which runs on an individual's computer, allowing him to verify and exchange ecoins with the emint, to send and receive ecoins from other individuals, and to manage his ecoins stored in the memory of his computer (column 3, lines 26-30)].

f. Referring to claim 9:

i. Turk further teaches:

(1) wherein the user's account has a data structure identifying the user and containing information identifying the data items stored therein [i.e., "client software" is a software application which runs on an individual's computer, allowing him to verify and exchange ecoins with the emint, to send and receive ecoins from other individuals, and to manage his ecoins stored in the memory of his computer (column 3, lines 26-30)].

g. Referring to claim 10:

i. Turk further teaches:

(1) wherein the information of each data item includes at least one of the type, size, time/date of submission, period of storage and pointers to the locations of the stored parts of the data item [i.e., the system of the invention requires some system users to establish a fiduciary relationship with a storage site. The relationship is confirmed when a system user either (1) stores gold with, or (2) purchases from another person gold already held at one or more storage sites. In the first case, the storage site verifies the receipt (in which time/date of submission is considered to include in this receipt) of the gold and provides confirmation to the system user specifying the pure weight, that is "size", and/or other physical attributes of the gold. In the second case, the storage site records the transfer of gold from one system user to the other (column 4, lines 50-59)].

h. Referring to claim 11:

i. Turk further teaches:

(1) wherein the means for encoding: a) divides the data item into a multiple of q K-tuples, denoted as $X_i = (x_{i1}, x_{i2} \dots x_{ik})$, $i = 1$ to q , where x is a symbol over $GF(2^m)$ with m being a positive integer; b) for $i = 1$ to q , encodes X_i into a codeword $Y_i = (y_{i1}, Y_{i2} \dots y_{iN})$ using an (N, K) error-control code C , where Y_{ij} is a symbol over $GF(2^m)$; c) rearranges Y_j , for $i = 1$ to q , into q -tuples Z_j , $(y_{1j} y_{2j} \dots y_{qj})$, for $j = 1$ to N ; and d) stores the Z_j , for $j = 1$ to N , as said parts [i.e., in one such method known as the RSA algorithm, encryption and decryption are accomplished by two mathematical equations which are related as inverses of each other. These equations are the private key, used by the issuing financial institution to digitally sign, or certify, a note, and the related public key, used by the recipient to determine and verify the existence of a valid signature on the note, whereby the above claimed limitation is considered to include in this RSA algorithm (column 1, lines 23-30)].

i. Referring to claim 12:

i. Turk further teaches:

(1) wherein the means for decoding: a) on inputting a data item identity, for $j = 1$ to N , reads $Z'_j = (y'_{1j} y'_{2j} \dots y'_{qj})$ from the locations where Z_j was stored, where Z_j , $j = 1$ to N , are the parts of the data item as identified; b) rearranges Z'_j , for $j = 1$ to N , into N -tuples $Y'_i = (y'_{i1}, Y'_{i2} \dots y'_{iN})$, for $i = 1$ to q ; c) decodes Y'_i using an error- and -erasu re-co rrec ti on decoder of the (N, K) code C to obtain $X'_j = (x'_{j1}, X'_{j2} \dots x'_{jK})$, for $i = 1$ to q ; and d) concatenates X'_j , for $i = 1$ to q to form the data item [i.e., in one such method known as the RSA algorithm, encryption and decryption are accomplished by two mathematical equations which are related as inverses of each other. These equations are the private key, used by the issuing financial institution to digitally sign, or certify, a note, and the related public key, used by the recipient to determine and verify the existence of a valid signature on the note, whereby the above claimed limitation is considered to include in this RSA algorithm (column 1, lines 23-30)].

j. Referring to claims 13, 15, and 16:

i. These claims have limitations that is similar to those of claim 12, thus they are rejected with the same rationale applied against claim 12 above.

k. Referring to claim 14:

i. This claim has limitations that is similar to those of claim 11, thus it is rejected with the same rationale applied against claim 11 above.

l. Referring to claim 17:

i. Turk further teaches:

(1) means for encryption of the data item [i.e., "encrypt" is to scramble data so as to prevent unauthorized reading. In addition, "public key" is a mathematical key which is available publicly and which is used to verify digital signatures created with the matching private key, and in the context of encrypted communications is used to decrypt electronic data which can only be encrypted using the matched private key (column 3, lines 55-60)];

m. Referring to claim 18:

i. Turk further teaches:

(1) wherein the user is able to instruct encryption, prior to encoding, of the data item to be stored during the transaction session [i.e., **these equations are the private key, used by the issuing financial institution to digitally sign, or certify, a note, and the related public key, used by the recipient, that is “the user”, to determine, that is “to instruct encryption”, and verify the existence of a valid signature on the note (column 1, lines 26-30)]**.

n. Referring to claim 19:

i. Turk further teaches:

(1) wherein the information of each data item includes an indication of whether or not the item is encrypted and a pointer to a decryption key [i.e., "ecoin" is the electronic representation of a valuable commodity, preferably, a precious metal such as gold, platinum, palladium, or silver, which is held for safekeeping at a storage site. Each ecoin comprises a unique serial number, a measure of the valuable commodity (for example, grams or ounces, and fractions thereof) that it represents, the name of a specific storage site where the valuable commodity is stored, and a date/time stamp of when the ecoin was created. Each ecoin may appear as a string of alphanumeric characters which may also be encrypted and/or digitally signed for security. (column 3, lines 41-52)].

o. Referring to claim 20:

i. This claim has limitations that is similar to those of claim 19, thus it is rejected with the same rationale applied against claim 19 above.

p. Referring to claims 21 and 24:

i. These claims have limitations that is similar to those of claim 18, thus they are rejected with the same rationale applied against claim 18 above.

q. Referring to claims 22 and 23:

i. Turk further teaches:

(1) wherein the means for checking decodes, checks and reencodes the data item at intervals; and wherein the intervals are of fixed

or variable period. [i.e., the RSA algorithm, that is “for checking decodes, checks and reencodes the data item at intervals” (column 1, line 24). In addition, “public key” is a mathematical key which is available publicly and which is used to verify digital signatures created with the matching private key, and in the context of encrypted communications is used to decrypt electronic data which can only be encrypted using the matched private key (column 3, lines 55-60)].

r. Referring to claim 25:

i. Turk further teaches:

(1) wherein the integrity check comprises a digital signature [i.e., “public key” is a mathematical key which is available publicly and which is used to verify, that is “the integrity check”, digital signatures created with the matching private key, and in the context of encrypted communications is used to decrypt electronic data which can only be encrypted using the matched private key (column 3, lines 55-60)].

s. Referring to claim 26:

i. This claim has limitations that is similar to those of claim 5, thus it is rejected with the same rationale applied against claim 5 above.

t. Referring to claim 27:

i. Turk further teaches:

(1) wherein communication with the user during the transaction session is by means of a plurality of messages each associated with a transaction to be performed [i.e., referring to Figure 1, “a plurality of messages each associated with a transaction to be performed” is considered to be sent to and from the storage site and the customers. Furthermore, the system of the invention requires some system users to establish a fiduciary relationship with a storage site. The relationship is confirmed when a system user either (1) stores gold with, or (2) purchases from another person gold already held at one or more storage sites. In the first case, the storage site verifies the receipt of the gold and provides confirmation to the system user specifying the pure weight and/or other

physical attributes of the gold. In the second case, the storage site records the transfer of gold from one system user to the other (column 4, lines 50-59)].

u. Referring to claims 28 and 29:

i. These claims have limitations that is similar to those of claim 27, thus they are rejected with the same rationale applied against claim 27 above.

v. Referring to claim 31:

i. This claim has limitations that is similar to those of claims 1 and 4, thus it is rejected with the same rationale applied against claims 1 and 4 above. In addition, Turk further teaches:

(1) receiving an instruction to retrieve a stored and encoded data item [i.e., the emint issue new ecoins and transmit them to the party requesting confirmation of ecoins, less the appropriate fees, whenever an ecoin is submitted for confirmation (column 6, lines 42-44). Furthermore, Using public key cryptography the emint digitally signs each ecoin with its private key, thus providing each ecoin with a Digital Hallmark.TM.. Blinding techniques may also be used to ensure the privacy of the user (the payer) of the ecoin. The Digital Hallmark.TM. allows an individual running the emint's client software to verify that an ecoin was in fact issued by the emint and is not a forgery (column 5, lines 13-18].

w. Referring to claim 32:

i. Turk further teaches:

(1) sending the retrieved data item to the user [i.e., the emint issue new ecoins and transmit them to the party requesting confirmation of ecoins, less the appropriate fees, whenever an ecoin is submitted for confirmation (column 6, lines 42-44)].

4. Claims 33 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Carroll (US 6,105, 131), and further in view of Yasukawa et al (US 5,999,622).

a. Referring to claim 33:

i. Carroll teaches:

(1) a data depository having data storage means for storing digital data electronically [i.e., referring to Figure 1, The secure server 12 includes a vault deposit server ("VDSI") 20 connected to a certification management system ("CMS") 24 and optionally a directory services 22 (column 4, lines 14-16)];

(2) providing for registration of users of the data depository, each user having an account with the depository [i.e., referring to Figure 1, a registration authority terminal 16 can be connected to the computer network 14, that is for "providing for registration of users of the data depository", and each user can have a personal vault, that is "an account with the depository", as shown in Figure 2]; and

(3) in response to a request from a user, opening a transaction session with the user in which the user and the depository authenticate each other and performing a transaction instructed by the user in respect of a digital data item, the transaction being selected by the user from a plurality of available transactions including storage of the item in or retrieval of the item from the depository [i.e., in Figure 4B, a new account request form illustrates a set of fields. The fields may include user specific information such as name, address, and telephone number, transaction information such as account type, fund transfer, and deposit method, and terminal information such as the storage location of the certificate. The session can be secured by using SSL communication. Secure session are indicated by an unbroken arrow in the lower left hand corner of the screen (column 7, lines 1-8)];

(4) wherein storage of the item includes encoding the item into a plurality of parts and storing the encoded parts separately in the data storage means, and retrieval of the item includes decoding the encoded item to retrieve the item from the separately stored parts, whereby the item is retrievable even if some of the parts are lost or corrupted [i.e., a system including a secure server and processes enabling operating system integration through virtual logon and user data

encrypted in "personal vaults" (column 1, lines 54-57). Furthermore, protection of data stored in a personal vault 40 includes encryption, digital signatures, and digital certificates (column 6, lines 6-7)].

ii. Although Caroll teaches the claimed subject matter, Caroll is silent about encrypting data/item into a plurality of parts or portions or segments and storing them separately in storage sites. On the other hand, Yasukawa teaches:

(1) The encrypted digital information is stored in a file, but individual segments of data which make up the file are encrypted according to some chosen encryption pattern. The data segments encrypted represent logical segments corresponding to an actual portion of the physical media on which the file is stored (e.g. sectors on a CD-ROM, hard disk, a memory block, etc). The encrypted information includes data indicating the original proprietor of the original digital information (i.e. the original file in which the digital information is stored) (column 3, lines 43-52).

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have applied the teaching of Yasukawa into Caroll's system since using more than one encryption scheme changes the "depth" of the encryption segment providing additional protection to a portion of valuable data (column 3, lines 59-62 of Yasukawa).

iv. The ordinary skilled person would have been motivated to:

(1) have applied the teaching of Yasukawa into Caroll's system because data is encrypted on a per-sector basis. Some portion of a sector comprising a file can be left unencrypted, speeding access since less decryption is required. Different files can utilize different encryption depth techniques, increasing protection against unauthorized decryption (column 1, lines 66-67 through column 2, lines 1-4 of Yasukawa).

c. Referring to claim 35:

i. Carroll further teaches:

(1) the step of checking, at intervals, the integrity of data items stored in the depository [i.e., referring to Figure 1, "the step of checking, at

intervals, the integrity of data items stored in the depository" is considered to include in the secure server 12].

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Turk (US 5,671,364) discloses a system and method for permitting gold or other commodities to circulate as currency requires a network of system users that participate in financial transactions where payment is made in units of gold (see abstract).

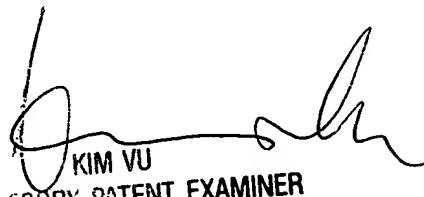
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

TBT

May 23, 2005



KIM VU
SUPERIOR PATENT EXAMINER
TECHNOLOGY CENTER 2100